

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY**

IN RE: AMERICAN MEDICAL  
COLLECTION AGENCY, INC.,  
CUSTOMER DATA SECURITY  
BREACH LITIGATION

*This Document Relates To:  
All Actions Against Laboratory Corporation  
of America Holdings*

Case No. 2:19-MD-02904-MCA-MAH

MDL 2904

**MEMORANDUM IN SUPPORT  
OF LABORATORY  
CORPORATION OF AMERICA  
HOLDINGS' MOTION TO  
DISMISS**

**Motion Date: July 5, 2022**

## **TABLE OF CONTENTS**

	<b>Page</b>
BACKGROUND.....	1
ARGUMENT .....	2
I. CERTAIN PLAINTIFFS STILL LACK ARTICLE III STANDING .....	2
A. Plaintiffs Have Not Shown A Causal Connection.....	3
B. Plaintiffs Have Not Alleged Article III Injury.....	6
II. PLAINTIFFS’ COMMON LAW CLAIMS FAIL.....	8
A. Multiple Plaintiffs’ Negligence and Negligence Per Se Claims Fail .....	8
1. Twelve Plaintiffs Fail to Allege that Labcorp Caused Cognizable Damages .....	8
2. Labcorp Did Not Owe Any Plaintiffs a Common Law Duty to Notify.....	10
3. Eighteen Plaintiffs’ Negligence Per Se Claims Fail.....	11
B. Plaintiffs’ Breach of Confidence Claim Should Be Dismissed .....	12
C. Plaintiffs’ Intrusion Upon Seclusion Claim Should Be Dismissed .....	14
D. Plaintiffs’ Unjust Enrichment Claim Should Be Dismissed .....	16
III. PLAINTIFFS’ STATUTORY CLAIMS SHOULD BE DISMISSED.....	18
A. Plaintiffs’ California Confidentiality of Medical Information Act Fails .....	18
B. Plaintiffs’ Statutory Claims Fail for Lack of Injury and Causation .....	23
1. Plaintiffs Fail to Allege Cognizable Injury .....	23
2. Plaintiffs Fail to Allege Causation.....	29
C. Plaintiffs’ Consumer Protection Act Claims Fail for Additional Reasons.....	30
1. Plaintiffs Cannot State a Claim Based on Alleged Misrepresentations or Omissions .....	30
a. Plaintiffs Fail to Plead Fraud or Deception with Particularity.....	31
b. Lack of Reliance or Likely Deception.....	31

c.	Plaintiffs’ Omission-Based Claims Fail Under Massachusetts and Wisconsin Law for Additional Reasons .....	33
2.	Plaintiffs’ Consumer Protection Claims Fail for Additional Reasons .....	33
a.	Plaintiffs’ UCL Claim Fails.....	33
b.	Plaintiffs’ Pennsylvania Consumer Protection Act Claim Fails .....	36
c.	Plaintiffs’ Kentucky Consumer Protection Law Claim Fails .....	36
d.	Plaintiffs Fail To Allege A Purchase Or Lease Under Three Statutes .....	37
D.	Plaintiffs’ State Data Breach Notification and Remaining Data Security Claims Should Be Dismissed .....	38
1.	Three State Statutes Have No Enforceable Private Right of Action .....	38
2.	Several Claims Fail Because the State Statute Does Not Apply Here.....	39
CONCLUSION .....		40

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>Acara v. Banks</i> , 470 F.3d 569 (5th Cir. 2006).....	34
<i>Allgood v. PaperlessPay Corp.</i> , 2022 WL 846070 (M.D. Fla. Mar. 22, 2022) .....	15
<i>In re Ambry Genetics Data Breach Litig.</i> , 2021 WL 4891610 (C.D. Cal. Oct. 18, 2021) .....	14
<i>Amburgy v. Express Scripts, Inc.</i> , 671 F. Supp. 2d 1046 (E.D. Mo. 2009) .....	11
<i>In re Anthem, Inc. Data Breach Litig.</i> , 162 F. Supp. 3d 953 (N.D. Cal. 2016) .....	13, 37
<i>Antman v. Uber Techs., Inc.</i> , 2015 WL 6123054 (N.D. Cal. Oct. 19, 2015).....	4, 29
<i>Arnold v. Microsoft Corp.</i> , 2000 WL 36114007 (Ky. Cir. Ct. July 21, 2000) .....	37
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009) .....	14
<i>Atlas Res., Inc. v. Liberty Mut. Ins. Co.</i> , 2010 WL 11552917 (D.N.M. Jun. 24, 2010) .....	23
<i>Attias v. CareFirst, Inc.</i> , 365 F. Supp. 3d 1, 5 (D.D.C. 2019).....	9, 24, 27, 29
<i>In re AZEK Bldg. Prod., Inc., Mktg. &amp; Sales Practices Litig.</i> , 82 F. Supp. 3d 608 (D.N.J. 2015) .....	36
<i>Barnett v. First Nat'l Bank of Omaha</i> , 2022 WL 627028 (W.D. Ky. Mar. 3, 2022).....	29
<i>Baysal v. Midvale Indem. Co.</i> , 2022 WL 1155295 (W.D. Wis. Apr. 19, 2022) .....	4, 6

<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	32
<i>Belmont v. MD Inv. Partners, Inc.</i> , 708 F.3d 470 (3d Cir. 2013) .....	36
<i>Benner v. Bank of Am., N.A.</i> , 917 F. Supp. 2d 338 (E.D. Pa. 2013) .....	28
<i>Berry v. Nat'l Med. Servs., Inc.</i> , 41 Kan. App. 2d 612 (2009) .....	38
<i>In re Brinker Data Incident Litig.</i> , 2020 WL 691848 (M.D. Fla. Jan. 27, 2020) .....	13, 14
<i>Broder v. Cablevision Sys. Corp.</i> , 418 F.3d 187 (2d Cir. 2005) .....	35
<i>Brush v. Miami Beach Health Care Grp.</i> , 238 F. Supp. 3d 1359 (S.D. Fla. 2017) .....	17
<i>C.C. v. Med-Data Inc.</i> , 2022 WL 970862 (D. Kan. Mar. 31, 2022) .....	8, 27
<i>Campbell v. Facebook Inc.</i> , 77 F. Supp. 3d 836 (N.D. Cal. 2014) .....	26
<i>Carlsen v. GameStop, Inc.</i> , 833 F.3d 903 (8th Cir. 2016) .....	8
<i>Carlson v. Coca-Cola Co.</i> , 483 F.2d 279 (9th Cir. 1973) .....	34
<i>Carlson v. The Gillette Co.</i> , 2015 WL 6453147 (D. Mass. Oct. 23, 2015) .....	33
<i>Candle v. Towers, Perrin, Forster &amp; Crosby, Inc.</i> , 580 F. Supp. 2d 273 (S.D.N.Y. 2008) .....	10
<i>Chambliss v. Carefirst, Inc.</i> , 189 F. Supp. 3d 564 (D. Md. 2016) .....	25, 27
<i>Clapper v. Amnesty Int'l USA</i> , 568 U.S. 398 (2013) .....	2

<i>Claridge v. RockYou, Inc.</i> , 785 F. Supp. 2d 855 (N.D. Cal. 2011) .....	38
<i>Cooper v. Bonobos, Inc.</i> , 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022) .....	6, 7
<i>Corona v. Sony Pictures Ent., Inc.</i> , 2015 WL 3916744 (C.D. Cal. Jun. 15, 2015) .....	29
<i>In re Donald J. Trump Casino Sec. Litig.-Taj Mahal Litig.</i> , 7 F.3d 357 (3d Cir. 1993) .....	20
<i>Dugas v. Starwood Hotels &amp; Resorts Worldwide, Inc.</i> , 2016 WL 6523428 (S.D. Cal. Nov. 3, 2016) .....	15, 28
<i>Eisenhower Med. Ctr. v. Super. Ct.</i> , 226 Cal. App. 4th 430 (2014) .....	19
<i>Farmer v. Humana, Inc.</i> , 2022 WL 732126 (M.D. Fla. Jan. 25, 2022) .....	13
<i>Fernandez v. Leidos, Inc.</i> , 127 F. Supp. 3d 1078 (E.D. Cal. 2015) .....	5
<i>Fero v. Excellus Health Plan, Inc.</i> , 236 F. Supp. 3d 735 (W.D.N.Y. 2017) .....	34
<i>Finstad v. Washburn Univ. of Topeka</i> , 845 P.2d 685 (Kan. 1993) .....	25
<i>Foster v. Health Recovery Servs., Inc.</i> , 493 F. Supp. 3d 622 (S.D. Ohio 2020) .....	14
<i>Fox v. Iowa Health Sys.</i> , 399 F. Supp. 3d 780 (W.D. Wis. 2019) .....	39
<i>Gaddy v. Long &amp; Foster Cos.</i> , 2022 U.S. Dist. Lexis 46657 (D.N.J. Mar. 15, 2022) .....	13
<i>Gardiner v. Walmart Inc.</i> , 2021 WL 2520103 (N.D. Cal. Mar. 5, 2021) .....	9
<i>In re Gen. Motors LLC Ignition Switch Litig.</i> , 257 F. Supp. 3d 372 (S.D.N.Y. 2017) .....	33

<i>In re Google Assistant Priv. Litig.</i> , 457 F. Supp. 3d 797 (N.D. Cal. 2020) .....	27
<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.</i> , 806 F.3d 125 (3d. Cir. 2015) .....	26
<i>In re Grand Theft Auto Video Game Consumer Litig. (No. II)</i> , 251 F.R.D. 139 (S.D.N.Y. 2008) .....	37
<i>Griffey v. Magellan Health Inc.</i> , 2021 WL 4427065 (D. Ariz. Sept. 27, 2021) .....	10, 31
<i>Grube v. Daun</i> , 563 N.W.2d 523 (Wis. 1997) .....	39
<i>Gupta v. Asha Enterprises, L.L.C.</i> , 27 A.3d 953 (N.J. App. Div. 2011) .....	25
<i>Hadley v. Kellogg Sales Co.</i> , 243 F. Supp. 3d 1074 (N.D. Cal. 2017) .....	35
<i>Hall v. Equifax Info. Servs. LLC</i> , 204 F. Supp. 3d 807 (E.D. Pa. 2016) .....	24
<i>Hammond v. Bank of N.Y. Mellon Corp.</i> , 2010 WL 2643307 (S.D.N.Y. Jun. 25, 2010) .....	24
<i>Hetzl v. JPMorgan Chase Bank, N.A.</i> , 2014 WL 7336863 (E.D.N.C. Dec. 22, 2014) .....	11
<i>Hodges v. Apple Inc.</i> , 2013 WL 4393545 (N.D. Cal. Aug. 12, 2013) .....	35
<i>Holmes, v. Countrywide Fin. Corp.</i> , 2012 WL 2873892 (W.D. Ky. July 12, 2012) .....	24, 25
<i>Irwin v. Jimmy John's Franchise, LLC</i> , 175 F. Supp. 3d 1064 (C.D. Ill. 2016) .....	18
<i>Joseph v. Nordstrom, Inc.</i> , 2016 WL 6917279 (C.D. Cal. Jun. 17, 2016) .....	24, 30
<i>Kamal v. J. Crew Grp., Inc.</i> , 918 F.3d 102 (3d Cir. 2019) .....	13

<i>Khan v. Children’s Nat’l Health Sys.</i> , 188 F. Supp. 3d 524 (D. Md. 2016) .....	8, 26
<i>Kimbriel v. ABB, Inc.</i> , 2019 WL 4861168 (E.D.N.C. Oct. 1, 2019) .....	28
<i>Krottner v. Starbucks Corp.</i> , 406 F. App’x 129 (9th Cir. 2010) .....	10
<i>L.S. v. Mount Olive Bd. of Educ.</i> , 765 F. Supp. 2d 648 (D.N.J. 2011) .....	12
<i>Laster v. T-Mobile USA, Inc.</i> , 407 F. Supp. 2d 1181 (S.D. Cal. 2005) .....	38
<i>Legg v. Leaders Life Ins. Co.</i> , 2021 WL 5772496 (W.D. Okla. Dec. 6, 2021) .....	7
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992) .....	3
<i>Madrid v. Perot Sys. Corp.</i> , 130 Cal. App. 4th 440 (2005) .....	33
<i>Morfin v. Accredited Home Lenders, Inc.</i> , 2010 WL 391838 (S.D. Cal. Jan. 26, 2010) .....	35
<i>Mount v. PulsePoint, Inc.</i> , 2016 WL 5080131 (S.D.N.Y. Aug. 17, 2016) .....	17
<i>Mueller v. Harry Kaufmann Motorcars, Inc.</i> , 859 N.W.2d 451 (Wis. Ct. App. 2014) .....	25
<i>Nichols v. Kansas Political Action Comm.</i> , 11 P.3d 1134 (Kan. 2000) .....	39
<i>O’Donnell v. United States</i> , 891 F.2d 1079 (3d Cir. 1989) .....	15
<i>O’Shea v. Littleton</i> , 414 U.S. 488 (1974) .....	19
<i>Pruchnicki v. Envision Healthcare Corp.</i> , 439 F. Supp. 3d 1226 (D. Nev. 2020) .....	10



<i>Randolph v. ING Life Ins. &amp; Annuity Co.</i> , 973 A.2d 702 (D.C. 2009) .....	15
<i>Reilly v. Ceridian Corp.</i> , 664 F.3d 38 (3rd Cir 2011) .....	6
<i>Rojas-Lozano v. Google, Inc.</i> , 159 F. Supp. 3d 1101 (N.D. Cal. 2016) .....	36
<i>In re Sci. Applications Int’l Corp. Backup Tape Data Theft Litig.</i> , 45 F. Supp. 3d 14 (D.D.C. 2014) .....	4, 5
<i>Shafran v. Harley–Davidson, Inc.</i> , 2008 WL 763177 (S.D.N.Y. Mar. 20, 2008) .....	25, 29
<i>Silcox v. State Farm Mut. Auto. Ins. Co.</i> , 2014 WL 7335741 (S.D. Cal. Dec. 22, 2014) .....	35
<i>Sonner v. Premier Nutrition Corp.</i> , 971 F.3d 834 (9th Cir. 2020) .....	34
<i>In re Sony Gaming Networks &amp; Customer Data Sec. Breach Litig.</i> , 903 F. Supp. 2d 942 (S.D. Cal. 2012) .....	25
<i>In re Sony Gaming Networks &amp; Customer Data Sec. Breach Litig.</i> , 996 F. Supp. 2d 942 (S.D. Cal. 2014) .....	26, 29
<i>Stein v. Sprint Corp.</i> , 22 F. Supp. 2d 1210 (D. Kan. 1998) .....	24
<i>Steinberg v. CVS Caremark Corp.</i> , 899 F. Supp. 2d 331 (E.D. Pa. 2012) .....	26
<i>Stengart v. Loving Care Agency, Inc.</i> , 990 A.2d 650 (N.J. 2010) .....	15
<i>In re SuperValu, Inc. Customer Data Sec. Breach Litig.</i> , 925 F.3d 955, 964-65 (8th Cir. 2019) .....	28
<i>Sutter Health v. Super Ct.</i> , 227 Cal. App. 4th 1546 (2014) .....	20, 23
<i>Tabler v. Panera LLC</i> , 2020 WL 3544988 (N.D. Cal. Jun. 30, 2020) .....	32

<i>TransUnion v. Ramirez</i> , 141 S. Ct. 2190 (2021) .....	6
<i>Von Grabe v. Sprint PCS</i> , 312 F. Supp. 2d 1285 (S.D. Cal. 2003) .....	38
<i>Watkins v. MGA Ent., Inc.</i> , 550 F. Supp. 3d 815 (N.D. Cal. 2021) .....	34
<i>Willey v. J.P. Morgan Chase, N.A.</i> , 2009 WL 1938987 (S.D.N.Y. July 7, 2009) .....	29
<i>Williams v. Williams</i> , 323 S.E.2d 463 (N.C. Ct. App. 1984) .....	17
<i>Willingham v. Glob. Payments, Inc.</i> , 2013 WL 440702 (N.D. Ga. Feb. 5, 2013) .....	10
<i>Wilson v. Rater8, LLC</i> , 2021 WL 4865930 (S.D. Cal. Oct. 18, 2021) .....	19
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.</i> , 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017) .....	24, 25
<i>Young v. Carran</i> , 289 S.W.3d 586 (Ky. Ct. App. 2008) .....	12
<i>In re Zappos.com, Inc. Customer Data Sec. Breach Litig.</i> , 2013 WL 4830497 (D. Nev. Sept. 9, 2013) .....	18

## **Statutes**

73 Pa. Stat. Ann. § 201-2(4) .....	36
Cal. Civ. Code § 56.05(i) .....	19
Cal. Civ. Code § 56.10(c)(3) .....	22, 23
Cal. Civ. Code § 56.101(a) .....	23
Cal. Civ. Code § 1761(d) .....	37
Cal. Civ. Code § 1780(a) .....	37
Cal. Civ. Code § 1782(a) .....	38

Kan. Stat. Ann. § 50-7a02(e) .....	39
Kan. Stat. Ann. § 50-7a02(g) .....	39
Kan. Stat. Ann. § 50-624(c) .....	37
Kan. Stat. Ann. § 50-626(a) .....	37
Ky. Rev. Stat. Ann. § 365.732(8).....	39
Ky. Rev. Stat. § 367.220(1) .....	30, 37
Md. Code Ann. Com. Law § 13-408 .....	29
Md. Code Ann. Com. Law § 14-3503 .....	40
Md. Code Ann. Com. Law § 14-3507 .....	39
Md. Code Ann. Com. Law § 14-3508 .....	39
Wis. Stat. Ann. § 134.98(3m)(b).....	39
Wis. Stat. Ann. § 134.98(4) .....	39
<b>Regulations and Rules</b>	
45 C.F.R. § 164.404 .....	40
45 C.F.R. § 164.410 .....	40
Fed. R. Civ. P. 9(b) .....	31

Plaintiffs’ First Amended Consolidated Class Action Complaint (“FAC”) does nothing to remedy the deficiencies that prompted this Court to dismiss most claims asserted in the Consolidated Class Action Complaint (“CAC”). ECF 283; ECF 319. To be sure, Plaintiffs’ FAC attempt to plead around those defects. But the FAC remains riddled with flaws. Among other failings, the FAC continues to allege injuries this Court already found to be insufficient and fails to correct numerous other defects the Court identified—from failure to allege actionable deception to claim-specific infirmities. The two new causes of action Plaintiffs assert, breach of confidence and intrusion upon seclusion, are equally flawed. These claims simply do not apply where, as here, there was no affirmative disclosure of the information at issue. Because Plaintiffs’ claims fail as a matter of law despite a second bite at the apple, they should be dismissed with prejudice.

### **BACKGROUND**

In dismissing all but three causes of action asserted in the CAC, the Court held that half the Plaintiffs “failed to establish their standing because they have failed to allege an injury-in-fact” and that numerous claims otherwise failed as a matter of law. *Op.*, at 23. The Court granted Plaintiffs leave to file to “cure the deficiencies identified.” *Id.* at 69. The relevant allegations in Plaintiffs’ FAC—which re-asserts three common law claims and fourteen statutory claims the Court dismissed and asserts two new common law claims—remain unchanged. Labcorp’s systems were not impacted by the AMCA Cyberattack. *See* FAC ¶ 2. Labcorp did not send AMCA

Plaintiffs’ financial information. *Id.* ¶ 71. Plaintiffs do not allege that their email addresses, passwords, or usernames were impacted in the AMCA Cyberattack. *Id.* ¶ 86. Nor do Plaintiffs plausibly allege that test codes, diagnosis codes, or other medical information relating to them were held in the affected AMCA database. *Id.* ¶¶ 14-40. And Plaintiffs still do not allege that they paid Labcorp anything for the services they used. *Id.* ¶ 71. Plaintiffs have similarly realleged injuries that this Court found insufficient to confer Article III standing, including “expenses to prevent future identity theft,” “substantial risk of future” identity theft, “diminished . . . ‘value’ of their Personal Information,” and the “benefit of their bargain.” *Op.*, at 17-20; *see* FAC ¶¶ 8, 9, 191, 307, 331, 349, 360, 387, 394, 405, 423.

## **ARGUMENT**

### **I. CERTAIN PLAINTIFFS STILL LACK ARTICLE III STANDING<sup>1</sup>**

Despite revamping their allegations, twelve Plaintiffs still fail to allege facts sufficient to show any Article III injury that is “fairly traceable to the challenged action” and “concrete, particularized, and actual or imminent.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013) (citation omitted). Specifically, Plaintiffs Lebon, Cuvillier, Judelsohn, Lassiter, Laufenberg, Nazemnikov, Rothwell, Scott, Thomas, Vazquez, and Wallach have not plausibly alleged that their purported harms are

---

<sup>1</sup> Labcorp reserves its right to challenge the standing of all Plaintiffs and reasserts for preservation purposes the grounds for dismissal argued in its prior motion to dismiss, *see* Labcorp’s Br., ECF 148-1, but does not re-argue those points here.

traceable to the AMCA Cyberattack, and setting aside these purported harms, the same plaintiffs—as well as Plaintiff Allende—cannot satisfy Article III’s injury requirements. *Op.*, at 17-20.

**A. Plaintiffs Have Not Shown A Causal Connection**

The Plaintiffs identified above have not alleged a “causal connection” tying their purported injuries to Labcorp’s alleged conduct for several reasons. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

Failure to allege injuries occurring after August 2018. Four Plaintiffs do not allege that their purported injuries occurred after the AMCA Cyberattack, as this Court held was required to establish cognizable injury traceable to the Cyberattack. *Op.*, at 20-21. Plaintiff Lebon “does not recall the details” of his alleged credit card fraud, including when it allegedly occurred. FAC ¶ 31. The same is true for Plaintiff Cuvillier, who alleges nothing about when she supposedly “had to close a credit card account and open a new one with a new number” and “experienced attempted theft of her highly confidential information” via spam calls. *Id.* ¶ 39. Plaintiffs Lassiter and Laufenberg likewise allege that their injuries occurred “in or around 2018,” but do not allege that their alleged injuries occurred after August 2018.<sup>2</sup> *Id.* ¶¶ 18 (Lassiter’s alleged injuries); 21 (Laufenberg’s alleged injuries); 2 (alleging the Cyberattack began in

---

<sup>2</sup> Plaintiff Laufenberg alleges that her harm occurred within the “Data Breach window” “in or around 2018.” FAC ¶ 21. But the FAC does not define the term “Data Breach window” and, consequently, Plaintiffs have not sufficiently alleged that Laufenberg’s harm post-dated the AMCA Cyberattack.

August 2018). Plaintiffs Lebon, Cuvillier, Laufenberg and Lassiter therefore cannot rely on any of these alleged injuries to establish Article III standing.

Failure to allege injuries traceable to the information allegedly affected in the AMCA Cyberattack. Plaintiffs Rothwell, Cuvillier, and Wallach allege injuries relating to spam or phishing emails and password compromises, *see* FAC ¶¶ 26, 33, 39, but these Plaintiffs do not allege that emails, passwords, or usernames were impacted in the AMCA Cyberattack. *See* FAC ¶¶ 6, 86. Nor do Plaintiffs attempt to allege how phishing emails or compromised passwords or usernames relate to data elements that **were** allegedly impacted. Plaintiffs therefore have not—and cannot—trace any alleged harms to the AMCA Cyberattack.<sup>3</sup> *See, e.g., Baysal v. Midvale Indem. Co.*, 2022 WL 1155295, at \*3 (W.D. Wis. Apr. 19, 2022) (no plausible allegations that identity theft “can be traced” to the data breach because the stolen information was insufficient to commit such theft); *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at \*11 (N.D. Cal. Oct. 19, 2015) (similar); *In re Sci. Applications Int’l Corp. Backup Tape Data Theft Litig.* (“SAIC”), 45 F. Supp. 3d 14, 31-32 (D.D.C. 2014) (similar).

Similarly, Plaintiffs Lassiter, Nazemnikov, Laufenberg, Scott, Thomas, Vazquez, and Judelsohn cannot trace alleged injuries related to payment card and bank account misuse to the AMCA Cyberattack. Plaintiffs do not allege facts showing that they provided such information to Labcorp or AMCA. If Labcorp had

---

<sup>3</sup> As discussed in Section II.B below, these Plaintiffs’ remaining alleged harms are not cognizable injuries under Article III, and they therefore lack standing.

such information, it would have had no need to send it to AMCA. And Plaintiffs do not say that they paid anything to Labcorp or AMCA. That is fatal. *See, e.g., SAIC*, 45 F. Supp. 3d at 31 (no Article III standing based on alleged unauthorized charges where no allegations that plaintiffs' financial information was stolen). Plaintiffs' cannot evade this pleading deficiency by pointing to generic references to the provision of "Personal Information" to AMCA. *See* FAC ¶¶ 18, 19, 21, 24, 30, 34, 38, 71. There are no factual allegations showing that payment or banking information for **these** Plaintiffs' was provided to AMCA or Labcorp or affected in the Cyberattack. *See Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. 2015) (no standing where plaintiff failed to allege information necessary to commit fraud was stolen).

Failure to allege dark web activity connected to the AMCA Cyberattack.

Plaintiffs cannot fall back on allegations about dark web activity to satisfy Article III. Such allegations are unavailing because there is no allegation that the information impacted in the AMCA Cyberattack is the same information allegedly available for sale on the dark web. First, Lassiter and Wallach allege that items of "personal information" **not** impacted by the AMCA Cyberattack—including passwords and email addresses—were found on a dark web marketplace. FAC ¶¶ 18, 33. Second, Plaintiffs Lebon, Cuvillier, Lassiter, Laufenberg, Rothwell, and Wallach (like the other named Plaintiffs) allege that their "personal information" was "discovered for sale on a dark web marketplace," without ever specifying what information was discovered or whether they provided it to Labcorp or AMCA. *See id.* ¶¶ 21, 26, 31, 39. Generic



allegations that unspecified information is on the dark web is insufficient to “plausibly allege a causal nexus” to the Cyberattack. *Op.*, at 21. Third, because no Plaintiff alleges when their “personal information” was discovered for sale on the dark web, Plaintiffs also cannot trace this alleged injury to the AMCA Cyberattack. *See id.*

### **B. Plaintiffs Have Not Alleged Article III Injury**

After setting aside alleged harms that are not traceable to the AMCA Cyberattack, Plaintiffs Lebon, Cuvillier, Judelsohn, Lassiter, Laufenberg, Nazemnikov, Rothwell, Scott, Thomas, Vazquez, and Wallach, as well as Plaintiff Allende, only allege injuries that this Court has already held are insufficient to show Article III injury. FAC ¶¶ 18, 21, 26, 31, 33, 39, 40, 191.

*First*, these Plaintiffs allege “mere risk of future harm,” which is “insufficient” to establish Article III standing. *Op.*, at 11, 18 (citing *TransUnion v. Ramirez*, 141 S. Ct. 2190, 2204, 2211 (2021); *see also Baysal*, 2022 WL 1155295, at \*3 (“[T]he threat of future, speculative harm cannot satisfy Article III standing without more.”)). None of these Plaintiffs allege the type of “particularized harm” the Court held is required to confer Article III standing. *Op.*, at 18; *see, e.g.*, FAC ¶¶ 31, 191.

*Second*, these Plaintiffs’ alleged mitigation efforts remain insufficient for Article III injury. *See, e.g.*, FAC ¶ 40, 191. The Court dismissed this theory of harm based on alleged “expenses to prevent future identity theft” without “particularized facts that would corroborate a fear of identity theft,” and the FAC adds no such alleged facts. *Op.*, at 17 (citing *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3rd Cir 2011)); *see also Cooper*

*v. Bonobos, Inc.*, 2022 WL 170622, at \*5 (S.D.N.Y. Jan. 19, 2022) (“[P]laintiffs ‘cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.’”).

*Third*, this Court also has already rejected Plaintiffs’ “benefit of the bargain” theory of injury where, as here, there are no allegations “that Plaintiffs’ Personal Information was of any material economic value with respect to the services Plaintiffs received from Defendants.” *Op.*, at 19; *see also* FAC ¶ 295. Plaintiffs still have not alleged that their information was of value to Labcorp with respect to the services they received. *See Op.*, at 19-20. And Plaintiffs still do not allege that they paid for Labcorp’s services. *See, e.g., Legg v. Leaders Life Ins. Co.*, 2021 WL 5772496, at \*7 (W.D. Okla. Dec. 6, 2021) (rejecting benefit of the bargain theory because plaintiff had not “indicated that he paid any sort of premium” for data security or that the breach “diminished the value of the [] products he received”).

*Fourth*, Plaintiffs’ assertion that they lost the “value of their privacy,” *see, e.g.*, FAC ¶ 231, is nothing more than an attempt to repackage the loss of value theory the Court rejected.<sup>4</sup> *Op.*, at 18-19. No facts alleged in the FAC show that Plaintiffs’ privacy “diminished [in] value because of alleged inadequate data security.” *Op.*, at 20. This Court should join the numerous other courts that have rejected vague

---

<sup>4</sup> To the extent Plaintiffs attempt to revive their loss of value of theory, *see* FAC ¶ 191, that effort fails too. To support such a theory, the Court held that Plaintiffs must allege that Labcorp “monetized” their personal information, *Op.*, at 19, but there are no such allegations in the FAC.

allegations about loss of privacy as insufficient to show injury in fact. *See, e.g., C.C. v. Med-Data Inc.*, 2022 WL 970862, at \*10 (D. Kan. Mar. 31, 2022) (plaintiff's "loss of privacy, in and of itself, is not a concrete harm" under Article III); *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 533 (D. Md. 2016) (same).

These Plaintiffs therefore lack Article III standing and should be dismissed.

## II. PLAINTIFFS' COMMON LAW CLAIMS FAIL<sup>5</sup>

### A. Multiple Plaintiffs' Negligence and Negligence Per Se Claims Fail

The negligence and negligence per se claims of twelve Plaintiffs should be dismissed because they have not alleged Labcorp's conduct caused cognizable damages. In addition, all Plaintiffs' negligence claims premised on a common law duty to notify should be dismissed because no such duty exists, and eighteen Plaintiffs' negligence per se claims fail for additional reasons.

#### 1. Twelve Plaintiffs Fail to Allege that Labcorp Caused Cognizable Damages

Damages are an essential element of negligence and negligence per se claims regardless of which state's law applies.<sup>6</sup> "[I]t is crucial . . . not to conflate" this requirement with "Article III's requirement of injury in fact," *Carlsen v. GameStop, Inc.*,

---

<sup>5</sup> Labcorp reserves all rights to raise at an appropriate juncture the choice of law considerations that the Court found to be premature at this stage. *See Op.*, at 23-25. While Labcorp believes those considerations show that the law of Plaintiffs' home states should apply to their claims, *see* Labcorp's Br., ECF 148-1, at 13-16, the Court need not engage in a choice of law analysis to dismiss Plaintiffs' claims because, as described below, they fail as a matter of law regardless of what state's law applies.

<sup>6</sup> *See* Labcorp's Br., ECF 148-5 (App. A summarizing negligence arguments).

833 F.3d 903, 909 (8th Cir. 2016), because the damages required to state a claim is a “higher” hurdle. *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 5 (D.D.C. 2019), *on reconsideration in part*, 518 F. Supp. 3d 43 (D.D.C. 2021). The allegations of harm for twelve Plaintiffs<sup>7</sup> do not clear that bar and should be dismissed.

That is especially true for Plaintiffs’ loss of value of privacy and benefit of the bargain theories of harm, which do not even satisfy Article III. *See supra* § I.B. Plaintiffs fail to allege facts showing that any purported loss of privacy amounted to actual damages. Nor do the allegations in the FAC show that Plaintiffs were denied any benefit of the bargain and thereby suffered damages. On the contrary, it is abundantly clear that Plaintiffs did *not* pay any consideration for the services from Labcorp, let alone pay “some amount attributable to data security.” *Gardiner v. Walmart Inc.*, 2021 WL 2520103, at \*6-7 (N.D. Cal. Mar. 5, 2021).

Plaintiffs’ other allegations regarding lost time spent mitigating issues related to the AMCA Cyberattack,<sup>8</sup> purported discovery of their “personal information” for sale on the dark web, and instances of data misuse and attempted fraudulent activity,<sup>9</sup> also

---

<sup>7</sup> Plaintiffs Buhr, Laufenberg, Haley, Rothwell, Kaplan, Lebon, Wallach, Wrenn, Thrower, Judelsohn, Cuvillier, and Allende.

<sup>8</sup> *See* FAC ¶¶ 20 (Buhr); 21 (Laufenberg); 22 (Haley); 26 (Rothwell); 27 (Kaplan); 31 (Lebon); 35 (Wrenn); 37 (Thrower); 38 (Judelsohn); 39 (Cuvillier); 40 (Allende).

<sup>9</sup> *See* FAC ¶¶ 20 (Buhr) (unsuccessful attempts to open credit cards, allegation that her credit report was hacked, and blocked attempted charges to her debt card); 22 (Haley) (received hard hits on her credit report); 26 (Rothwell) (uptick in phishing emails and unsuccessful extortion email); 27 (Kaplan) (credit was pulled); 33 (Wallach) (attempts to change passwords on accounts); 35 (Wrenn) (prevented credit card inquiry, failed attempts to open accounts in her name); 37 (Thrower) (unauthorized

do not clear the lower Article III hurdle and all involve potential future risks, not actual damages. *See, e.g., Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 284 (S.D.N.Y. 2008) (courts “have uniformly ruled” that time and expense combatting increased risk of future identity theft is not “an injury that the law is prepared to remedy”); *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1232 (D. Nev. 2020) (“Injuries that stem from the danger of future harm are insufficient to support a negligence action.”); *Griffey v. Magellan Health Inc.*, 2021 WL 4427065, at \*5 (D. Ariz. Sept. 27, 2021) (attempted fraud amounts to “a threat of future injuries” that is not cognizable); *Krottner v. Starbucks Corp.*, 406 F. App’x 129, at 131 (9th Cir. 2010) (no damages where opening of unauthorized bank account did not result in unauthorized charges).

2. Labcorp Did Not Owe Any Plaintiffs a Common Law Duty to Notify

Plaintiffs’ negligence claims based on an alleged duty to provide “timely and adequate notice of the Data Breach,” FAC ¶ 229, fail as a matter of law. In refusing to create such a duty, courts note that numerous data breach notification statutes already exist, many of which lack a private right of action. *See Willingham v. Glob. Payments, Inc.*, 2013 WL 440702, at \*18 (N.D. Ga. Feb. 5, 2013) (no common law

---

credit inquiries); 38 (Judelsohn) (attempt to clone his credit card, failed attempt to charge his credit card); 39 (Cuvillier) (closed credit card, increased spam calls); 40 (Allende) (no allegation). The remaining two Plaintiffs, Laufenberg and Lebon, FAC ¶¶ 21, 31, fail to connect their harms to the AMCA Cyberattack because they do not specifically allege **when** the purported harms took place. *See* § I.A *supra*.

notice requirement outside of data breach statute); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009) (no cause of action “in negligence or otherwise” for alleged inadequate notice and court would “not create a claim where one does not exist”). Thus, regardless of the applicable state law, Plaintiffs’ negligence claims based on an alleged duty to notify should be dismissed.

### 3. Eighteen Plaintiffs’ Negligence Per Se Claims Fail

The negligence per se claims of 18 Plaintiffs<sup>10</sup> should be dismissed because across the potentially applicable states either (1) no such claim is recognized, or (2) it cannot be premised on alleged violation of Section 5 of the FTC Act or HIPAA.

*First*, as the Court previously held, four states—Arkansas, California, Maryland, and Massachusetts—do not recognize negligence per se as an independent cause of action. *Op.*, at 32-33.<sup>11</sup> That holding applies with equal force to the FAC.

*Second*, this Court also held that the laws of six other states do not allow a claim for negligence per se based on statutes without a private right of action, like HIPAA and Section 5 of the FTC. *Id.*<sup>12</sup> That includes North Carolina law, *see Hetzel v.*

*JPMorgan Chase Bank, N.A.*, 2014 WL 7336863, at \*7 (E.D.N.C. Dec. 22, 2014), which

---

<sup>10</sup> Palmer; Lassiter; Nazemnikov; Buhr; Laufenberg; Rothwell; Kaplan; Shulman; Spencer; Thomas; Lebon; Gadero; Wallach; Vazquez; Harris; Thrower; and Judelsohn. Labcorp reserves its right to challenge the remaining negligence per se claims, including on the basis that negligence per se is not a proper cause of action under applicable law.

<sup>11</sup> *See* FAC ¶¶ 17 (Arkansas); 18-19 (California); 27 (Maryland); 28 (Massachusetts).

<sup>12</sup> *See Id.* ¶¶ 20-21 (Florida); 26 (Kentucky); 29-30 (Mississippi); 31 (New Jersey); 32-33 (New York); 34-35 (North Carolina); 36-37 (Ohio); and 38 (Pennsylvania).

Plaintiffs assert should apply to all putative class members' negligence per se claims. FAC ¶ 202. The same is true for New Jersey and Kentucky. *See L.S. v. Mount Olive Bd. of Educ.*, 765 F. Supp. 2d 648, 652 (D.N.J. 2011) ("Plaintiffs' claims [for negligence per se] under . . . HIPAA are dismissed because . . . HIPAA do[es] not provide for a private right of action."); *Young v. Carran*, 289 S.W.3d 586, 588-89 (Ky. Ct. App. 2008) (holding that negligence per se claims based on violations of federal law, including HIPAA specifically, are impermissible). The FAC again includes only vague and conclusory allegations that Labcorp violated HIPAA and Section 5 of the FTC Act, which are the sole bases for Plaintiffs' negligence per se claims. FAC ¶¶ 232-46. Thus, whether the applicable law is that of North Carolina or the home states of these Plaintiffs, the outcome is the same: Plaintiffs cannot pursue a negligence per se claim based on alleged violation of HIPAA or Section 5 of the FTC Act. The negligence per se claims for these eighteen Plaintiffs should be dismissed with prejudice.

#### **B. Plaintiffs' Breach of Confidence Claim Should Be Dismissed**

As a threshold and wholly dispositive issue, four of the sixteen states at issue in the FAC—including North Carolina—do not appear to even recognize breach of confidence as a cause of action, and an additional two states only recognize breach of confidence in trade secret matters, mandating dismissal of this cause of action under

the law of any of these states.<sup>13</sup> *See* Fanning Certif., App. A. For the remaining ten states, Plaintiffs’ claim still fails because breach of confidence requires “the unconsented, unprivileged disclosure to a third party of nonpublic information.”

*Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019); *see also* App. A.<sup>14</sup>

“Disclosure” necessitates ***affirmative action*** on the part of the discloser. *See, e.g., In re Brinker Data Incident Litig.*, 2020 WL 691848, at \*22 (M.D. Fla. Jan. 27, 2020)

(“[D]isclosure” is an “act or process.”); *cf. In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 1002-03 (N.D. Cal. 2016) (“[I]n order to “disclose” something, the information holder must commit some affirmative, voluntary act.”).

As a result, numerous courts have held that information stolen from a party in a cyberattack does not constitute “disclosure” to support a breach of confidence claim. *See, e.g., Farmer v. Humana, Inc.*, 2022 WL 732126, at \*7 (M.D. Fla. Jan. 25, 2022) (no breach of confidence claim “where a defendant’s inadequate security facilitated the theft of information by third-parties.” (internal quotations omitted)); *In re Brinker Data Incident Litig.*, 2020 WL 691848, at \*22 (dismissing breach of confidence claim because defendant “did not do any act that made Plaintiffs’ information known—the information was stolen by third-parties”); *Gaddy v. Long & Foster Cos.*, 2022 U.S. Dist.

---

<sup>13</sup> Labcorp is not aware of an Arkansas, Kentucky, Maryland, or North Carolina case recognizing such a claim. Nor is Labcorp aware of a Kansas or Texas case recognizing such a claim outside of the trade secret context.

<sup>14</sup> There are other state-specific reasons why Plaintiffs’ breach of confidence cause of action fails, and Labcorp expressly reserves these arguments.



Lexis 46657, at \*31 (D.N.J. Mar. 15, 2022) (same); *In re Ambry Genetics Data Breach Litig.*, 2021 WL 4891610, at \*8 (C.D. Cal. Oct. 18, 2021) (same); *Foster v. Health Recovery Servs., Inc.*, 493 F. Supp. 3d 622, 635 (S.D. Ohio 2020) (same).

The same is true here. No facts alleged in the FAC show that Labcorp affirmatively disclosed Plaintiffs' information to the threat actors behind the AMCA Cyberattack. Nor can Plaintiffs state a breach of confidence claim based on Labcorp's "disclosure" of information to AMCA, as Plaintiffs allege no facts showing that transmission of information to AMCA for purposes of collecting debts was an unconsented to and unlawful disclosure to a third party. Plaintiffs cannot escape these flaws by simply repeating the word "disclosure," *see* FAC ¶¶ 248-251, which is an unadorned, naked assertion insufficient under *Ashcroft v. Iqbal*, 556 U.S. 662 (2009). Indeed, Plaintiffs' assertion that an "unauthorized disclosure occurred" because Labcorp "failed to implement and maintain reasonable safeguards" sounds "in negligence not breach of confidence." *In re Brinker Data Incident Litig.*, 2020 WL 691848, at \*22. Plaintiffs' claim for breach of confidence should be dismissed.

### **C. Plaintiffs' Intrusion Upon Seclusion Claim Should Be Dismissed**

Plaintiffs' intrusion upon seclusion claim fails for similar reasons. Across the potentially applicable state laws, intrusion upon seclusion requires an *intentional* act—an intrusion into the private matters of another. *See* Fanning Certif., App. B. For this reason, courts hold that alleged negligent conduct is insufficient, and regularly dismiss intrusion upon seclusion claims in cases, like here, where a third party stole

the data. *See, e.g., Allgood v. PaperlessPay Corp.*, 2022 WL 846070, at \*12 (M.D. Fla. Mar. 22, 2022); *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 711 (D.C. 2009).

Plaintiffs have not and cannot allege facts showing that Labcorp—as opposed to the threat actors here—intentionally invaded their privacy. *See e.g., Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at \*12 (S.D. Cal. Nov. 3, 2016) (no allegations that data breach was “an intentional violation” of plaintiff’s privacy).

Plaintiffs try to elide this precedent by asserting in conclusory fashion that Labcorp “disclos[ed]” their information “without permission” to a third party purportedly “unequipped and unable” to keep it secure, which “enabl[ed]” the “disclosure” of that information. FAC ¶¶ 254-255. This contortion about supposedly impermissible disclosures that enabled other disclosures is not the intentional act that the claim requires. As the Third Circuit has made clear, “an actor commits an intentional intrusion [upon seclusion] only if he believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act.” *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989). Plaintiffs do not allege that Labcorp believed it lacked—or actually lacked—the legal authority to collect unpaid bills by using debt collections services. On the contrary, Plaintiffs allege that Labcorp charges for services it provides to patients, and when Plaintiffs did not pay for those services, Labcorp refers the unpaid bills to AMCA. FAC ¶¶ 17-40, 48-50.

Plaintiffs also cannot meet another required element that cuts across potentially applicable state laws: the intrusion must be at least highly offensive. *See, e.g., Stengart v.*

*Loving Care Agency, Inc.*, 990 A.2d 650, 659 (N.J. 2010); *see also* Fanning Certif., App. B.

Plaintiffs do not allege facts showing that sending information to a debt collector after non-payment is a highly offensive intrusion into their private affairs. The threat actors' alleged access to information held by a debt collector does not transform Labcorp's transfer of data to that debt collector into an intentional and offensive intrusion.

#### **D. Plaintiffs' Unjust Enrichment Claim Should Be Dismissed**

Plaintiffs' unjust enrichment claim fares no better. The Court previously dismissed this cause of action because Plaintiffs "allege[d] no facts showing that Defendants h[ad] been enriched." *Op.*, at 33. In particular, the CAC contained "no facts showing how Defendants reaped monetary benefits or otherwise profited from Plaintiffs' Personal Information." *Id.* at 34. The FAC suffers from the same fundamental flaw. Plaintiffs allege that because of Labcorp's purported deceptive conduct, it was able to sell "more services than it otherwise would have," "charging for and collecting for those services." FAC ¶ 266. But there still are no allegations in the FAC that these ***Plaintiffs*** (or anyone else) paid Labcorp for any services, regardless of what services Plaintiffs received or what Labcorp charged. *See id.* ¶¶ 17-40. Despite four plaintiffs alleging they received collection notices from AMCA, *see id.* ¶¶ 21, 23, 31, 40, ***none*** allege they paid anything. Nor are there allegations that Labcorp received "any additional value" for Plaintiffs' information. *Op.*, at 34. Claims that Plaintiffs used Labcorp's services and had their information sent to

AMCA for failure to pay for those services does not show enrichment.

Plaintiffs' claim also should be dismissed because (1) Plaintiffs have not alleged that any supposed enrichment came at their expense, and (2) to the extent any enrichment occurred, Plaintiff have not sufficiently alleged that it was unjust. No facts alleged in the FAC show that Plaintiffs suffered any detriment.<sup>15</sup> On the contrary, Plaintiffs obtained services from Labcorp without paying for those services. Nor do Plaintiffs allege that after providing information to Labcorp they could no longer use or monetize that information. *See Mount v. PulsePoint, Inc.*, 2016 WL 5080131, at \*6 (S.D.N.Y. Aug. 17, 2016) (rejecting unjust enrichment claim based on alleged misappropriation of the value of plaintiffs' information), *aff'd*, 684 F. App'x 32 (2d Cir. 2017), *as amended* (May 3, 2017).

Likewise, even if Labcorp received some benefit at Plaintiffs' expense, any enrichment was not unjust. *See Williams v. Williams*, 323 S.E.2d 463, 465 (N.C. Ct. App. 1984) (finding enrichment as the expense of another is insufficient, as "[t]here must be some added ingredients to invoke the unjust enrichment doctrine." (citation omitted)). Labcorp provided healthcare services to Plaintiffs, and no Plaintiffs alleges that they did not receive such services. *See e.g., Brush v. Miami Beach Health Care Grp.*, 238 F. Supp. 3d 1359, 1369 (S.D. Fla. 2017) (no unjust enrichment where plaintiff "transacted to receive healthcare services from the Defendants—not data security

---

<sup>15</sup> *See* Labcorp's Br., ECF 148-8 (App. D – Column: Basis for Recover: Enrichment was at Plaintiff's Expense).

services”); *Irwin v. Jimmy John’s Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016) (similar). Any benefit conferred on Labcorp was fairly received in exchange for the services provided to each Plaintiff. FAC ¶¶ 14-42; see e.g., *In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, 2013 WL 4830497, at \*5 (D. Nev. Sept. 9, 2013) (no unjust enrichment where plaintiffs “bestowed the benefit of their purchase . . . [and] [d]efendant provided [p]laintiffs a benefit in return (providing the goods)”).

### **III. PLAINTIFFS’ STATUTORY CLAIMS SHOULD BE DISMISSED**

#### **A. Plaintiffs’ California Confidentiality of Medical Information Act Fails**

Plaintiffs’ statutory claims suffer from the same fundamental flaws that led this Court to dismiss them before, starting with Plaintiffs’ California Confidentiality of Medical Information Act (“CMIA”) claim. The Court previously held that Plaintiffs failed to allege facts sufficient to show that their “medical information” was viewed or accessed by an unauthorized person as required under the CMIA. *Op.*, at 63-64. Plaintiffs’ renewed CMIA claim suffers from the same defect and should be dismissed again. Plaintiffs’ claim also should be dismissed for a reason the Court did not need to reach before: the statute expressly authorizes health providers like Labcorp to disclose medical information to billing entities and does not impose liability based on the recipient entities’ subsequent conduct.

This Court correctly held that the CAC “fail[ed] to allege that ‘medical information,’ as contemplated by the CMIA, was stolen.” *Op.*, at 63. As the Court

explained, “the information allegedly compromised . . . is not the type of information protected by the CMIA,” *id.* at 64, which is limited to information “regarding a patient’s medical history, mental or physical condition, or treatment.” *Id.* at 63; Cal. Civ. Code § 56.05(i). “Absent factual allegations that the information compromised involved Plaintiffs’ medical history and treatment programs, [Plaintiffs] fail to state a claim for relief under the CMIA.” *Op.*, at 64; *see also Wilson v. Rater8, LLC*, 2021 WL 4865930, at \*5 (S.D. Cal. Oct. 18, 2021) (finding treating physician names, medical treatment appointment information, and medical treatment discharge dates and times were not “substantive” medical information under the CMIA).

The FAC does not allege facts showing that the ***named Plaintiffs***’ medical information was compromised; nor does it allege that medical information for the ***named Plaintiffs*** was provided by Labcorp to AMCA or stored in AMCA’s affected Champ database. *See* FAC ¶ 18 (alleging that Labcorp only provided Plaintiff Lassiter’s “personal information”<sup>16</sup> to AMCA); FAC ¶ 19 (same, as to Plaintiff Nazemnikov). That is fatal. *See, e.g., O’Shea v. Littleton*, 414 U.S. 488, 494 (1974)

---

<sup>16</sup> Plaintiffs define “Personal Information” as “protected health information . . . and personally identifiable information . . . such as . . . names, mailing addresses, phone numbers, dates of birth, Social Security numbers (“SSNs”), information related to Plaintiffs’ and Class Members’ medical providers and services (such as dates of service and referring doctor) and other private information, such as credit and debit card numbers, bank account information, insurance, and insurance subscriber identification numbers.” FAC ¶ 6. This information is ***not*** “medical information” under the CMIA. *See Op.*, at 63-64 (“Personal Information” allegedly impacted is not “medical information”); *Eisenhower Med. Ctr. v. Super. Ct.*, 226 Cal. App. 4th 430, 435-36 (2014); *Wilson*, 2021 WL 4865930, at \*5.

(plaintiff who cannot assert a claim against defendant may not “seek relief on behalf of himself or any other member of the class”).

Ignoring these foundational flaws, the FAC nonetheless implausibly and summarily alleges that “medical information compromised included . . . information related to Plaintiff’s and California Subclass members’ medical treatment, such as tests ordered, ordering physician, and ICD [diagnostic] Codes.” FAC ¶ 277. The FAC does not allege facts showing how medical information could have been compromised—let alone viewed or accessed<sup>17</sup>—for the named Plaintiffs when the information that Labcorp sent to AMCA to facilitate collections did not include their medical information, and Plaintiffs never allege that such information for Labcorp patients was held in the affected Champ database.

What is more, the notification letters Plaintiffs allege they received from Labcorp, *see* FAC ¶¶ 18-19, confirm that the data transmitted to AMCA to facilitate collections, which was stored in AMCA’s Champ database, ***did not*** include medical information.<sup>18</sup> *See* Fanning Certif., Ex. 1, Sample Labcorp Notice Letter (July 20,

---

<sup>17</sup> Plaintiffs must plead not only that their medical information was compromised, but also that it was “improperly viewed or otherwise accessed.” *Sutter Health v. Super Ct.*, 227 Cal. App. 4th 1546, 1558 (2014) (“That the records have changed possession even in an unauthorized manner does not mean they have been exposed to the view of an unauthorized person.”).

<sup>18</sup> At least 26 Plaintiffs allege that they received a data breach notification letter from Labcorp but Plaintiffs do not attach those letters to the FAC. *See* FAC ¶¶ 11-41. The Court may consider an “undisputedly authentic document that a defendant attaches as an exhibit to a motion to dismiss if the plaintiff’s claims are based on the document” without converting the motion into one for summary judgment. *In re Donald J. Trump*

2019) (“No ordered tests, laboratory test results, or diagnostic information were in the AMCA affected system.”).

Plaintiffs try to elide these flaws and manufacture a CMIA claim in two ways. First, they cite documents that suggest Labcorp had the option of providing customers’ health or medical information to AMCA. *See* FAC ¶ 59 (citing an AMCA-Labcorp agreement that allows for the possibility that medical information could be provided to AMCA); *id.* ¶ 60 (citing an AMCA-Labcorp agreement addendum that allegedly includes oversight mechanisms for protected health information though not necessarily “medical information”); *id.* ¶ 62 (citing AMCA’s suggested list of billing placement data elements, which in any event did not include “medical information” under the CMIA). But whether Labcorp **could** have sent AMCA medical information for the named Plaintiffs does not plausibly show that it **did** so, particularly when the other allegations in the FAC suggest that Labcorp did not.

Second, Plaintiffs cite documents that contain information about tests ordered and diagnostic codes. *See* FAC ¶ 2 n.1. Critically, nothing in the FAC connects this information to the named Plaintiffs. *Id.* The information also is **separate** from the files that Labcorp generated from its billing system when referring unpaid bills for collection, FAC ¶ 50, which in turn, were stored in AMCA’s affected Champ database. *See* FAC ¶¶ 61, 77. Indeed, there are no allegations that these files, or any

---

*Casino Sec. Litig.-Taj Mahal Litig.*, 7 F.3d 357, 368 n.9 (3d Cir. 1993) (quotations omitted).



similar document or information gleaned from them, was ever stored in the affected Champ database. *Id.*; *see also* FAC ¶ 62 (citing AMCA email attaching requisition PDFs for a non-Plaintiff customer).

At bottom, Plaintiffs' CMIA claim is predicated on discrete documents that have nothing to do with the named Plaintiffs and are at odds with the FAC's allegations about what data Labcorp sent to AMCA in the regular course (not medical information) and what data was housed in the Champ database (not medical information). *See* FAC ¶ 61 ("LabCorp provided AMCA with Personal Information regarding LabCorp's patients in order to facilitate the bill-collection process."). Plaintiffs still have not plausibly alleged that their medical information was impacted, and their CMIA claim should be dismissed for this reason.

Even if Plaintiffs' medical information was impacted (and it was not), their CMIA claim still fails for additional reasons the Court did not reach before: (1) Labcorp's provision of information to AMCA for billing purposes was expressly authorized by the statute, and (2) AMCA's subsequent actions or omissions do not amount to disclosure under the CMIA and cannot otherwise create liability for Labcorp. First, Plaintiffs cannot overcome the CMIA's express authorization for a health provider—which Plaintiffs allege that Labcorp is, *see* FAC ¶ 274—to disclose medical information to an "entity that provides billing, claims management, medical data processing, or other administrative services." Cal. Civ. Code § 56.10(c)(3). Labcorp's release of information to AMCA, a billing services provider, was clearly

permissible under the plain language of the statute. *Id.*

Second, the statute provides that this information “shall not be further disclosed by the recipient,” *id.*, and the recipient, AMCA, did not affirmatively “disclose” the information to the threat actors. *Sutter Health*, 227 Cal. App. 4th at 1556 (explaining that “disclosure” under Section 56.10 requires an “affirmative communicative act,” which does not occur if the information is stolen). Moreover, nowhere does the CMIA impose liability for a health provider based on subsequent actions or omissions of a billing service recipient. *See, e.g., Atlas Res., Inc. v. Liberty Mut. Ins. Co.*, 2010 WL 11552917, at \*7 (D.N.M. Jun. 24, 2010) (highlighting that the CMIA “expressly permits disclosure” to certain entities, including those “that provide billing . . . services”). Nor does the statute provide that a health provider has a duty to protect the systems of a third party. *Cf.* Cal. Civ. Code § 56.101(a) (imposing requirements on a health provider to preserve the confidentiality of information that *it holds*). This Court should reject Plaintiffs’ invitation to read additional duties into the statute where the California legislature and state courts have not done so.

## **B. Plaintiffs’ Statutory Claims Fail for Lack of Injury and Causation**

### **1. Plaintiffs Fail to Allege Cognizable Injury**

Plaintiffs’ other statutory claims based on nine consumer protection laws and four notification and data security statutes require them to show that they suffered

actual harm. All but one named Plaintiff fails to satisfy this essential requirement.<sup>19</sup>

*Future Risk.* Plaintiffs’ allegations of an “imminent and significant risk of identity theft, financial fraud, and other identity theft into the indefinite future,” *see, e.g.,* FAC ¶ 7, are “not sufficient to allege ‘lost money or property’” as many states require.<sup>20</sup> *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at \*22 (N.D. Cal. Aug. 30, 2017) (dismissing California Unfair Competition Law (“UCL”) claim).<sup>21</sup> This “hypothetical” harm also is not sufficiently “quantifiable or measurable” to qualify as “ascertainable loss”<sup>22</sup> or satisfy other states’ “actual injury” or damages requirements.<sup>23</sup> Allegations that Plaintiffs’ “personal information” was

---

<sup>19</sup> The Court previously found that Massachusetts Plaintiff Shulman alleged sufficient injuries under the state consumer protection statute. Labcorp reserves all rights to challenge this conclusion on appeal, and through further litigation, but does not move to dismiss Plaintiff Shulman’s statutory claim on this basis. As discussed below, the Court should again dismiss Shulman’s claim to the extent it is based on alleged deceptive misrepresentations and omissions. *See Op.*, at 59.

<sup>20</sup> *Joseph v. Nordstrom, Inc.*, 2016 WL 6917279, at \*3 (C.D. Cal. Jun. 17, 2016) (California Consumer Legal Remedies Act (“CLRA”) requires “economic injury”).

<sup>21</sup> This Court held that Plaintiff Nazemnikov’s UCL claim failed because he had not adequately alleged reliance or that Labcorp had correspondingly benefitted. *See Op.*, at 57-58. The Court also noted that Plaintiff Nazemnikov failed to plead “a likelihood of redressable future harm,” but did not squarely address whether a risk of future harm could satisfy the UCL. *Id.* at 58. It cannot.

<sup>22</sup> *Holmes, v. Countrywide Fin. Corp.*, 2012 WL 2873892, at \*11, \*14 (W.D. Ky. July 12, 2012) (finding no injury under Kentucky law’s “ascertainable loss” requirement); *Hall v. Equifax Info. Servs. LLC*, 204 F. Supp. 3d 807, 812 (E.D. Pa. 2016) (dismissing Pennsylvania claim absent “an actual, non-speculative, loss of money or property”).

<sup>23</sup> *Hammond v. Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, at \*12-13 (S.D.N.Y. Jun. 25, 2010) (dismissing New York and California claims based on “increased risk of identity theft”); *Attias*, 365 F. Supp. 3d at 13 (same under Maryland law); *Stein v. Sprint Corp.*, 22 F. Supp. 2d 1210, 1216 (D. Kan. 1998) (Kansas requires that plaintiff “suffered an injury”), *on reconsideration* (Aug. 27, 1998).

“discovered for sale on a dark web marketplace” is insufficient as well. FAC ¶¶ 18, 19, 25-28, 32, 33, 38, 40; *In re Yahoo!*, 2017 WL 3727318, at \*22 (allegations that data found for sale on dark web “is not sufficient to allege ‘lost money or property’ under the UCL”).

*Mitigation.* Plaintiffs’ allegations that they spent time reviewing credit statements or monitoring their credit, *see* FAC ¶¶ 18, 19, 25, 26, 27, 28, 32, 33, 38, 40, and that some purchased or otherwise obtained password or credit monitoring services, FAC ¶¶ 17, 18, 33, are not enough for Article III standing, *Op.*, at 14, much less states’ statutory injury requirements. Indeed, “[i]n the context of data breach litigation, courts have consistently held that a plaintiff may not use mitigation costs alone to establish a cognizable injury in fact.” *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 571 (D. Md. 2016). Regardless of the applicable injury requirement—whether economic injury or damages,<sup>24</sup> ascertainable loss,<sup>25</sup> pecuniary loss,<sup>26</sup> or actual damages or injury<sup>27</sup>—voluntary mitigation measures against speculative, future harm are insufficient.

---

<sup>24</sup> *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 966 (S.D. Cal. 2012) (mitigation measures insufficient under the UCL and CLRA).

<sup>25</sup> *Holmes*, 2012 WL 2873892, at \*11, \*14 (“time” monitoring credit and credit monitoring fees not “ascertainable loss[es]” under Kentucky law); *see also Gupta v. Asha Enterprises, L.L.C.*, 27 A.3d 953, 960 (N.J. App. Div. 2011) (“cost of cure” allegations insufficient unless underlying injury is a “loss of moneys or property”).

<sup>26</sup> *Compare Mueller v. Harry Kaufmann Motorcars, Inc.*, 859 N.W.2d 451, 459 (Wis. Ct. App. 2014) (Wisconsin requires “monetary loss”) *with* FAC ¶ 40 (not alleging any).

<sup>27</sup> *Shafraan v. Harley–Davidson, Inc.*, 2008 WL 763177, at \*2-3 (S.D.N.Y. Mar. 20, 2008) (finding “time and money . . . spent to guard against identity theft,” including credit

*Privacy.* This Court has already held that Plaintiffs’ alleged loss of the “value of their” information, FAC ¶ 191(a); *see also id.* ¶ 307, 331, 349, 360, 394, 405, 423, does not rise to the level of an Article III injury. *Op.*, at 19; *see also In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 149, 152 (3d. Cir. 2015) (rejecting loss of value theory where plaintiffs did not allege “that they ever participated or intended to participate in” any market for their information or that defendant “prevented them from capturing the full value” of that information). Courts have similarly dismissed loss of value and related loss of privacy allegations as insufficient to show “ascertainable loss,”<sup>28</sup> actual damages,<sup>29</sup> or “economic injury.”<sup>30</sup>

*Benefit of the Bargain.* Plaintiffs’ allegations that they have lost “the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant’s [alleged] violations” also fail. *See* FAC ¶¶ 295, 307, 331, 349, 360, 394, 405, 423. The Court has already dismissed this theory in the context of Article III standing, *Op.*, at

---

monitoring, were not cognizable injuries under New York law); *Finstad v. Washburn Univ. of Topeka*, 845 P.2d 685, 691 (Kan. 1993) (consumer must be “aggrieved,” by an invasion of their “legal right” or a direct effect on their “pecuniary interest”).

<sup>28</sup> *Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 339 (E.D. Pa. 2012) (noting that Pennsylvania law requires an “ascertainable loss of money or property” and rejecting “loss of the value” of PII as sufficient injury).

<sup>29</sup> *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1003-1004 (S.D. Cal. 2014) (neither loss of value of PII nor loss of privacy qualify as “actual harm” under New York law); *Khan*, 188 F. Supp. 3d at 533-34 (rejecting both loss of value and loss of privacy).

<sup>30</sup> *See Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014) (loss of value of PII and loss of privacy are not injuries under the UCL).

19,<sup>31</sup> and it should do the same here with respect to Plaintiffs’ statutory claims. The FAC still does not allege that “Plaintiffs’ Personal Information was of any material economic value with respect to the services Plaintiffs received,” *id.*; nor is this type of injury cognizable where Plaintiffs did not pay for the services they received. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 834 (N.D. Cal. 2020) (“[I]t cannot be said that Plaintiffs received less than what they paid for—they appeared to have paid nothing”). And, in any case, Plaintiffs have not alleged that the value of the services they received was diminished by the AMCA Cyberattack.<sup>32</sup>

*Alleged Data Misuse.* In addition to the speculative harms discussed above, certain Plaintiffs allege forms of potential identity theft, such as unauthorized credit card transactions and unsolicited emails. None of these allegations show cognizable injury under Plaintiffs’ respective state consumer protection acts.

Five Plaintiffs allege unauthorized bank account, credit, or debit charges, *see* FAC ¶¶ 18 (Lassiter), 19 (Nazemnikov), 25 (Finch), 32 (Gadero); 38 (Judelsohn),<sup>33</sup> but

---

<sup>31</sup> Indeed, Plaintiffs alleged that AMCA “did not need to access Plaintiffs’ PHI to collect payments.” FAC ¶ 131.

<sup>32</sup> *See Chambliss*, 189 F. Supp. 3d at 572 (benefit of the bargain theory “is consistently rejected in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach”); *see also Med-Data Inc.*, 2022 WL 970862, at \*9 (similar); *Attias*, 365 F. Supp. 3d at 13, *on reconsideration in part*, 518 F. Supp. 3d 43 (D.D.C. 2021) (rejecting Plaintiffs’ benefit of the bargain theory).

<sup>33</sup> These Plaintiffs bring claims under California, Kansas, New York, and Pennsylvania law. Other Plaintiffs, *see, e.g.*, FAC ¶ 30 (Thomas), also fail to allege actual loss from unauthorized charges, but they reside in states under whose laws Plaintiffs do not assert consumer protection act claims.

none assert that they lost any money as a result of the unauthorized charges. *See id.* Indeed, there is no “reasonable [inference]” of any economic loss in such circumstances because “federal law and card-issuer contracts ordinarily absolve the consumer from any obligation to pay the fraudulent charge.” *In re SuperValu, Inc. Customer Data Sec. Breach Litig.*, 925 F.3d 955, 964-65 (8th Cir. 2019) (such allegations insufficient to show “actual damages” under consumer protection statutes); *Dugas*, 2016 WL 6523428, at \*4 (unauthorized but reimbursed charges did not satisfy as “loss of money or property” under California UCL); *Benner v. Bank of Am., N.A.*, 917 F. Supp. 2d 338, 360 (E.D. Pa. 2013) (plaintiff must “point to money or property that he would have had but for” the attempted fraud to sustain a claim under the Pennsylvania statute).<sup>34</sup> Similarly, Plaintiff Kaplan has not alleged any out-of-pocket expenses or other loss as a result of the alleged credit card inquiries. *See* FAC ¶ 27; *Kimbriel v. ABB, Inc.*, 2019 WL 4861168, at \*3 (E.D.N.C. Oct. 1, 2019) (credit inquiries not an injury-in-fact because they did not “plausibly show that plaintiffs’ compromised data is being used or that future use . . . is ‘certainly impending’”).

Plaintiffs’ remaining injury allegations are likewise unavailing. New York Plaintiff Wallach alleges that there were attempts to change her passwords, FAC ¶ 33, but Plaintiffs do not allege that passwords were impacted in the AMCA Cyberattack, and these allegations also boil down to “a perceived risk of future injury” that is not

---

<sup>34</sup> *See also* Labcorp’s Br., ECF 148-9 (App. E – injury required for California, New York, and North Carolina statutes).



cognizable under New York law. *Shafran*, 2008 WL 763177, at \*3; *see also Willey v. J.P. Morgan Chase, N.A.*, 2009 WL 1938987 at \*9 (S.D.N.Y. July 7, 2009). Plaintiff Rothwell’s allegation that he received “threatening phishing emails”—another data element not alleged to be impacted by the Cyberattack, *see supra* § I.B—does not rise to an “ascertainable loss of money or property” under the Kentucky Consumer Protection Act. *Barnett v. First Nat’l Bank of Omaha*, 2022 WL 627028, at \*8 (W.D. Ky. Mar. 3, 2022). Plaintiff Kaplan’s allegation that she “received alerts from fraud monitoring products” is insufficient under the Maryland Consumer Protection Act, FAC ¶ 27, because she does not allege an “identifiable loss” as the statute requires. *Attias*, 365 F. Supp. 3d at 13.

*Notification.* Plaintiffs’ state data breach notification and data security claims also require a showing of actual injury. *See, e.g.,* Md. Code Ann. Com. Law § 13-408; *In re Sony*, 996 F. Supp. 2d at 1010 (“[A] plaintiff must allege actual damages flowing from the unreasonable delay.”). These claims should be dismissed because Plaintiffs do not allege injury caused by any alleged deficiency in notification—FAC ¶¶ 18, 19, 25, 26, 27, 40—as opposed to the AMCA Cyberattack generally. *See, e.g., Corona v. Sony Pictures Ent., Inc.*, 2015 WL 3916744, at \*5 (C.D. Cal. Jun. 15, 2015) (dismissing breach notification claim for failure to allege injury from deficient notice); *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at \*11 (N.D. Cal. Oct. 19, 2015) (same).

## 2. Plaintiffs Fail to Allege Causation

As with Plaintiffs’ common law claims, causation is an essential element of each



of Plaintiffs' state consumer protection act claims, *see, e.g., Joseph*, 2016 WL 6917279, at \*3 (California UCL); Ky. Rev. Stat. § 367.220(1); *see also* Labcorp's Br., ECF 148-9 (App. E chart summarizing consumer protection law arguments), and state data breach notification or security claims, *see supra* § III.B. And for the same reasons that certain Plaintiffs cannot satisfy Article III's traceability requirement, *see supra* § I.A, their statutory claims should also be dismissed for failure to allege that Labcorp caused any of Plaintiffs' alleged injuries.<sup>35</sup>

### **C. Plaintiffs' Consumer Protection Act Claims Fail for Additional Reasons**

In addition to failing to satisfy injury and causation requirements, Plaintiffs' statutory claims suffer from additional deficiencies that merit dismissal.

#### **1. Plaintiffs Cannot State a Claim Based on Alleged Misrepresentations or Omissions**

This Court dismissed several consumer protection act claims in the CAC for failure to plead that Plaintiffs relied on or were otherwise misled by any actionable misrepresentation or omission. *See Op.*, at 56-57, 60. In the FAC, Plaintiffs' consumer protection claims are primarily based on Labcorp's purported failure to disclose that it did not reasonably secure Plaintiffs' information, ensure its vendors reasonably secured such information, or comply with certain legal obligations. *See*

---

<sup>35</sup> FAC ¶¶ 18 (Lassiter); 19 (Nazemnikov); 21 (Laufenberg); 24 (Scott); 26 (Rothwell); 30 (Thomas); 31 (Lebon); 33 (Wallach); 34 (Vazquez); 38 (Judelsohn); 39 (Cuvillier).

FAC ¶¶ 294, 305, 327, 347, 359, 393, 403, 422.<sup>36</sup> These statutory claims fail as a matter of a law for several reasons.

a. *Plaintiffs Fail to Plead Fraud or Deception with Particularity*

As this Court held, Plaintiffs’ allegations of “misrepresentation and knowing omissions” must meet Rule 9(b)’s heightened pleading standard. *See Op.*, at 40-41. Plaintiffs, however, still fail to identify any specific misrepresentation or omission made to them by Labcorp. For example, Plaintiff Shulman “believes she reviewed Labcorp’s privacy policies,” but fails to state what those policies said and what part of those policies contains alleged misrepresentations or omissions. FAC ¶ 28. *See, e.g., Griffey*, 2021 WL 4427065, at \*13 (dismissing claim because plaintiff failed to explain “how or why [defendant’s] policy was misleading, noncompliant, or inadequate”). Because the FAC does not even cite Labcorp’s alleged statements, Plaintiffs’ misrepresentation and omission-based claims fall far short of Rule 9(b)’s requirements. *See Op.*, at 40.

b. *Lack of Reliance or Likely Deception*

This Court previously dismissed Plaintiffs’ CLRA, UCL, Pennsylvania, and New York statutory claims for failure to plead that they “read any data privacy

---

<sup>36</sup> Plaintiffs appear to have abandoned their theory that Labcorp misrepresented its oversight of AMCA, instead relying upon allegations that Labcorp did not disclose “that it did not reasonably ensure its billing collector AMCA adequately secured patients’ Personal Information.” FAC ¶¶ 294, 305, 327, 347, 359, 393, 403, 422. Nevertheless, any allegations that could arguably support a theory of misrepresentation fail as well.

policies before purchasing medical services.” Op., at 61. Plaintiffs Rothwell, Judelsohn, and Allende still do not allege they read any such policies, *see* FAC ¶ 26, 38, 40, and Plaintiffs Nazemnikov, Gadero, Shulman, and Wallach’s allegations that each “does not recall” if he or she reviewed a privacy policy, or is not certain or merely “believes” he or she did, is insufficient under the California, Massachusetts, and New York statutes.<sup>37</sup> FAC ¶¶ 19, 28, 32, 33; *see Tabler v. Panera LLC*, 2020 WL 3544988, at \*6-7 (N.D. Cal. Jun. 30, 2020) (dismissing UCL and CLRA claims for failure to allege specific facts regarding statements); *see also* Labcorp’s Br., ECF 148-9 (App. E).

Plaintiffs’ omission-based allegations further fail because none of the Plaintiffs allege they would not have used Labcorp’s services if they had known about the purported omissions. *See, e.g.*, FAC ¶ 18. Instead, Plaintiffs merely allege they would not “have ***continued*** to use” Labcorp services had they been informed that Labcorp was going to share information with AMCA. *See, e.g., id.* (emphasis added). This theory implies that Plaintiffs anticipated that they would both use Labcorp’s services on multiple occasions and that their information would be sent to a debt collection agency after those subsequent visits because they did not intend to pay for Labcorp’s services when they received them. Plaintiffs do not allege sufficient facts to support this attenuated causal chain, nor is it plausible to assume it. *Twombly*, 550 U.S. at 557.

---

<sup>37</sup> Indeed, an inference that any of these Plaintiffs actually reviewed the policies is not “plausible” when they do not allege when this review happened or anything about what the policies said. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007).

That is particularly true because several Plaintiffs allege that they did *not* knowingly use Labcorp's services; their doctors transferred their samples to Labcorp without Plaintiffs' advance knowledge. *See* FAC ¶¶ 19, 21, 25, 27, 32, 33, 38, 40.

c. *Plaintiffs' Omission-Based Claims Fail Under Massachusetts and Wisconsin Law for Additional Reasons*

Plaintiffs' omission-based claims also fail under the Massachusetts and Wisconsin statutes because Wisconsin does not permit omission-based claims, *see In re Gen. Motors LLC Ignition Switch Litig.*, 257 F. Supp. 3d 372, 456 (S.D.N.Y. 2017), and Massachusetts law only prohibits "material, knowing, and willful nondisclosure." *See Carlson v. The Gillette Co.*, 2015 WL 6453147, at \*6 (D. Mass. Oct. 23, 2015). Plaintiffs have not alleged that Labcorp knowingly committed any fraudulent omissions because they have not alleged facts showing Labcorp had actual knowledge of AMCA's allegedly deficient data security.

2. Plaintiffs' Consumer Protection Claims Fail for Additional Reasons

a. *Plaintiffs' UCL Claim Fails*

The Court previously held that Plaintiffs are not entitled to restitution or injunctive relief under the UCL, Op. at 58, the only available remedies. *See Madrid v. Perot Sys. Corp.*, 130 Cal. App. 4th 440, 452 (2005). Nothing in the FAC has changed, and Plaintiffs' UCL claim should be dismissed on that basis alone. Plaintiffs still do not allege any "benefit to [Labcorp]" as required to be entitled to restitutionary relief under the UCL. Op., at 58. Nor does the FAC add any allegations to show "a

likelihood of redressable future harm” as also required to “justify injunctive relief,” *id.*, much less any allegations showing that Plaintiffs lack an adequate remedy at law. *See Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020) (affirming dismissal of a UCL claim because the complaint failed to allege that the plaintiff lacked adequate legal remedies); *Watkins v. MGA Ent., Inc.*, 550 F. Supp. 3d 815, 818 (N.D. Cal. 2021) (collecting post-*Sonner* cases dismissing UCL claims where plaintiffs failed to allege they lacked an adequate remedy at law).

In addition to this threshold flaw, Plaintiffs’ attempts to assert “unlawful” and “unfair” conduct under the UCL fall flat. As to unlawfulness, that theory should be rejected for two reasons. First, Plaintiffs’ UCL claim cannot be predicated on Labcorp’s alleged failure to comply with the FTC Act and HIPAA, *see* FAC ¶ 290, because these statutes have no private right of action and instead include detailed administrative enforcement mechanisms that preclude private enforcement. *See, e.g., Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 777 (W.D.N.Y. 2017) (rejecting claim predicated on FTC Act and HIPAA); *see also Acara v. Banks*, 470 F.3d 569, 571 (5th Cir. 2006) (“HIPAA limits enforcement of the statute to the Secretary of Health and Human Services.”); *Carlson v. Coca-Cola Co.*, 483 F.2d 279, 280 (9th Cir. 1973) (“[T]he Act vests initial remedial power solely in the Federal Trade Commission.”).<sup>38</sup>

---

<sup>38</sup> Plaintiffs’ UCL claims also cannot be based on alleged violation of the CLRA or California Records Act, *see* FAC ¶¶ 290, 298-309, because as shown in this Section and § III.C *supra*, each of those claims is fundamentally flawed and should be dismissed.

The Court should not allow Plaintiffs to circumvent these remedial schemes and “thwart” legislative intent through the backdoor of a consumer protection statute. *Broder v. Cablevision Sys. Corp.*, 418 F.3d 187, 199 (2d Cir. 2005). Second, Labcorp’s alleged failure to comply with unnamed “common law” or “statutory duties,” *see* FAC ¶ 290, is too conclusory and indefinite to support a UCL claim. *See, e.g., Hodges v. Apple Inc.*, 2013 WL 4393545, at \*6 (N.D. Cal. Aug. 12, 2013) (to support an “unlawful” theory “a plaintiff must identify the particular section of the statute” and plead with particularity how it was allegedly violated).

With respect to unfairness, Plaintiffs cannot base that theory on Labcorp’s purported fraudulent or unlawful conduct because as shown above Plaintiffs have not alleged facts showing that Labcorp committed any actionable misrepresentation or omission or violated any statute that can provide a basis for liability. *See* §§ III.B-C; *Hadley v. Kellogg Sales Co.*, 243 F. Supp. 3d 1074, 1104 (N.D. Cal. 2017) (“unfair” theory fails where underlying allegations overlap with allegations insufficient to show fraudulent or unlawful conduct). The remaining allegations in the FAC amount to bald conclusions of law, *see* FAC ¶ 291, and do not show that Labcorp’s purported conduct was unfair. *See Silcox v. State Farm Mut. Auto. Ins. Co.*, 2014 WL 7335741, at \*5 (S.D. Cal. Dec. 22, 2014). Indeed, Labcorp’s alleged failure to stop the actions of two third parties—AMCA and the attackers—cannot be considered unfair. *See, e.g., Morfin v. Accredited Home Lenders, Inc.*, 2010 WL 391838, at \*7 (S.D. Cal. Jan. 26, 2010)

(dismissing plaintiff's unfairness claim absent allegations that defendant participated in the challenged conduct).

Plaintiffs' assertion that Labcorp violated legislatively-declared public policy articulated in HIPAA and the FTC Act, among other statutes, fails as well. *See* FAC ¶ 290. Plaintiffs cite no "established public policy" that Labcorp purportedly violated by virtue of having a business associate targeted in a cyberattack. *See, e.g., Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1118 (N.D. Cal. 2016) (rejecting unfairness claim where plaintiff failed to cite a "specific" law supporting the asserted policy at issue).

b. *Plaintiffs' Pennsylvania Consumer Protection Act Claim Fails*

This Court previously dismissed Plaintiffs' claim under the Pennsylvania statute for failure "to show actual reliance on [Labcorp's] allegedly wrongful conduct." Op., at 60. As shown above, because Plaintiff Judelsohn still does not allege he "viewed any data privacy policies before obtaining services" from Labcorp, his claim should be dismissed again. *Id.*; FAC ¶ 38. Plaintiffs' claim also fails for two additional reasons. First, Plaintiffs do not allege facts showing that Labcorp misrepresented the characteristics or quality of any "good" or "services" as the statute requires. *See* 73 Pa. Stat. Ann. § 201-2(4); *Belmont v. MD Inv. Partners, Inc.*, 708 F.3d 470, 498 (3d Cir. 2013). Second, the economic loss rule bars the claim. *See In re AZEK Bldg. Prod., Inc., Mktg. & Sales Practices Litig.*, 82 F. Supp. 3d 608, 622 (D.N.J. 2015).

c. *Plaintiffs' Kentucky Consumer Protection Law Claim Fails*

Plaintiffs still do not satisfy the Kentucky statute's territoriality requirements

either,<sup>39</sup> which limit claims to three locations: (1) the Circuit Court in which the seller resides or “is doing business”; (2) the Circuit Court in which the purchaser . . . resides; or (3) “where the transaction in question occurred.” Ky. Rev. Stat. Ann. § 367.220(1). Plaintiffs do not allege that Labcorp resides in Kentucky. Nor has the sole Kentucky Plaintiff, Rothwell, filed an underlying lawsuit in any Kentucky court or alleged that any “transaction” occurred outside of the state and in New Jersey.

The Kentucky statute also prohibits class actions. *See Arnold v. Microsoft Corp.*, 2000 WL 36114007, at \*6 (Ky. Cir. Ct. July 21, 2000), *aff’d*, 2001 WL 1835377 (Ky. Ct. App. Nov. 21, 2001). Federal courts have dismissed class action claims on that basis, and so should this Court. *See In re Anthem*, 162 F. Supp. 3d at 999-1001 (dismissing claim with prejudice); *In re Grand Theft Auto Video Game Consumer Litig. (No. II)*, 251 F.R.D. 139, 160 (S.D.N.Y. 2008) (finding that statute did not support class actions).

d. *Plaintiffs Fail To Allege A Purchase Or Lease Under Three Statutes*

Plaintiffs’ CLRA, Kansas, and Kentucky claims each also fail because Plaintiffs do not allege they purchased or leased any service or good, as each statute requires. *Compare* Cal. Civ. Code §§ 1780(a), 1761(d); Kan. Stat. Ann. §§ 50-626(a), 50-624(c); Ky. Rev. Stat. Ann. § 367.220(1) *with* FAC ¶¶ 18, 19, 25, 26.<sup>40</sup> As Plaintiffs

---

<sup>39</sup> Labcorp reserves its right to challenge Plaintiffs’ Massachusetts consumer protection claim on territoriality grounds. *See Op.*, at 60 n.56.

<sup>40</sup> Plaintiffs’ CLRA fails for another independent reason: Plaintiffs did not satisfy the statute’s pre-suit notice requirement because the notice: (i) was sent the day before the CAC was filed—not at least thirty days prior, as required; (ii) was not sent by certified



acknowledge, they did not purchase anything from Labcorp: AMCA had their data because “LabCorp utilized [it] to collect unpaid bills.” FAC ¶ 50. Plaintiffs’ claims under these statutes should be dismissed on this basis. *See, e.g., Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 864 (N.D. Cal. 2011) (dismissing CLRA claim where plaintiff did not “purchase or lease” services); *Berry v. Nat’l Med. Servs., Inc.*, 41 Kan. App. 2d 612, 622 (2009) (dismissing claim where plaintiff did not “exchange anything of value” with defendants to secure their services”), *aff’d*, 292 Kan. 917 (2011).

#### **D. Plaintiffs’ State Data Breach Notification and Remaining Data Security Claims Should Be Dismissed**

Plaintiffs’ data breach notification and data security statutory claims also fail as a matter of law. As a threshold matter, Plaintiffs’ claims under the Kansas and Kentucky statutes should be dismissed because Plaintiffs previously conceded that these claims are without merit and withdrew them. *See* ECF 166 at 51. These claims, and Plaintiffs’ other claims under data security and notification statutes, also fail because Plaintiffs do not plead cognizable injury and causation, *see supra* § III.B, and for additional statute-specific reasons.

##### **1. Three State Statutes Have No Enforceable Private Right of Action**

---

or registered mail; (iii) did not identify particular CLRA violations; and (iv) did not demand that Labcorp correct or rectify specific alleged violations. *See* Cal. Civ. Code § 1782(a); *see also Von Grabe v. Sprint PCS*, 312 F. Supp. 2d 1285, 1304 (S.D. Cal. 2003) (dismissing claim with prejudice where the pre-suit notice insufficient); *Laster v. T-Mobile USA, Inc.*, 407 F. Supp. 2d 1181, 1196 (S.D. Cal. 2005), *aff’d*, 252 F. App’x 777 (9th Cir. 2007) (“Strict adherence to the [CLRA’s] notice provision is required.”).

Plaintiffs' claims under the Kansas and Wisconsin statutes fail because neither contains an express private cause of action, *see* Kan. Stat. Ann. § 50-7a02(g); Wis. Stat. Ann. § 134.98(4), and no such right can be implied under state law when neither "the language" nor "the form of the statute evinces the legislature's intent to create a private right of action." *Grube v. Daun*, 563 N.W.2d 523, 526 (Wis. 1997); *see also Nichols v. Kansas Political Action Comm.*, 11 P.3d 1134, 1143 (Kan. 2000) (same); *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 800 (W.D. Wis. 2019) (no indication Wisconsin legislature intended to create private right of action).

Likewise, Plaintiffs' claim under the Maryland law should be dismissed because the statute is explicit that alleged violations are only enforceable under the state consumer protection law, *see* Md. Code Ann. Com. Law § 14-3508, and, as shown above, that claim fails. *See supra* §§ III.B-C.

## 2. Several Claims Fail Because the State Statute Does Not Apply Here

Plaintiffs' claims under the Kansas and Kentucky statutes also fail because those laws expressly exempt entities regulated by HIPAA, *see* Kan. Stat. Ann. § 50-7a02(e); Ky. Rev. Stat. Ann. § 365.732(8), and Plaintiffs allege that Labcorp is subject to HIPAA. *See* FAC ¶¶ 51-58.

With respect to the Maryland and Wisconsin laws, those statutory requirements are inapplicable where, as here, Labcorp complied with federal notification requirements. *See* Md. Code Ann. Com. Law § 14-3507; Wis. Stat. Ann. §

134.98(3m)(b). While Plaintiffs again assert that the notice was “deficient,” FAC ¶¶ 141-142, they still have not and cannot allege specific shortcoming in the timing of the notices under federal law. AMCA sent a first batch of notices, FAC ¶ 140, consistent with applicable regulations. *See* 45 C.F.R. §§ 164.404, 164.410. And Plaintiffs say they received Labcorp notices in June or July, FAC ¶¶ 17-40, consistent with notice under 45 C.F.R. § 164.404. As to purported “deficiencies” in the content, Plaintiffs’ assertion that each letter did not specify “exactly” what information was affected, that the toll-free number was not operational for longer than 90-days, and that complimentary credit monitoring was not offered to everyone is beside the point, *see* FAC ¶ 141, because no allegations in the FAC show that the notices failed to contain the elements actually required by HIPAA. *See* 45 C.F.R. § 164.404(c)(1).

Finally, Plaintiffs’ claim under the Maryland statute also fails because it permits Labcorp to disclose personal information to nonaffiliated third party service providers like AMCA. Md. Code Ann. Com. Law § 14-3503. In particular, the statute does not require that the disclosing entity *itself* maintain the security of those third-party systems, but instead it “require[s] by contract that *the third party* implement and maintain reasonable security procedures and practices.” *Id.* (emphasis added). Plaintiffs do not allege facts showing that Labcorp failed to satisfy this requirement.

### CONCLUSION

For all the foregoing reasons, Labcorp respectfully requests that the Court grant its motion to dismiss Plaintiffs’ claims with prejudice.

Dated: May 31, 2022

By: /s/ Edward J. Fanning, Jr.

Edward J. Fanning, Jr., Esq. (055351994)

**McCARTER & ENGLISH, LP**

Four Gateway Center

100 Mulberry St.

Newark, NJ 07102

Telephone: (973) 622-4444

Facsimile: (973) 624-7070

Email: [efanning@mccarter.com](mailto:efanning@mccarter.com)

Allison Holt Ryan

Adam A. Cooke

Alicia J. Paller

**HOGAN LOVELLS US LLP**

555 Thirteenth Street, NW

Washington, DC 20004

Telephone: (202) 637-5600

Facsimile: (202) 637-5910

Email: [allison.holt-ryan@hoganlovells.com](mailto:allison.holt-ryan@hoganlovells.com)

[adam.a.cooke@hoganlovells.com](mailto:adam.a.cooke@hoganlovells.com)

[alicia.paller@hoganlovells.com](mailto:alicia.paller@hoganlovells.com)

*Counsel for Defendant Laboratory Corporation of  
America Holdings*